On the Transitive Substitution Groups whose Order is a Power of a Prime Number.

By G. A. Miller.

In a transitive group G of degree n, the subgroup G_1, which contains all the substitutions of G that do not involve a given letter, is of degree $n-\alpha$ ($\alpha \overline{>} 1$), and G_1 is one of n/α conjugate substitutions of G.* Each of these subgroups is, therefore, transformed into itself by αg_1 substitutions of G, g_1 being the order of G_1. These substitutions constitute a group G_2 of order αg_1. When $\alpha > 1$, G_2 contains a constituent of degree α. Since each of the substitutions of G_2 that is not contained in G_1 contains the α letters which G_1 omits, and since the order of G_2 is αg_1, it follows that the said constituent of G_2 is a regular group of order α. In what follows we shall assume that the order G is a power of a prime p^m. As the order of a subgroup G must be a power of the same prime $\alpha g_1 = p^{k'}$; hence, $\alpha = p^k$. This result may be stated as follows:

Theorem I.—*If the order of a transitive group is a power of a prime p^m, the subgroup formed by all its substitutions which omit a given letter omits p^k ($k \overline{>} 1$) letters of the group.*

Any set of conjugate subgroups or substitutions of G is transformed by all the substitutions of G according to a transitive substitution group of order p^β. Hence, Theorem I includes the theorem that all the substitutions of G which transform one of these subgroups or substitutions into itself, must also transform p^k ($k \overline{>} 1$) of its conjugates into themselves. In other words, the substitutions of G which transform one of a set of conjugate subgroups or substitutions into itself constitute a group in which p^k of these conjugates are invariant.† This includes the theorems. Every non-invariant subgroup or substitution of a group of order

*Cf. Netto, "Theory of Substitutions," 1892, p. 84. Also Cauchy, Comptes Rendus, vol. 21, 1845, p. 669.

† Burnside, "Theory of Groups," 1897, p. 65.

p^m is transformed into itself by p^k ($k \overline{>} 1$) of its conjugates. A group of order p^{m-1} that is contained in a group of order p^m is invariant. A group of order p^m cannot be generated by one set of its conjugate subgroups.

Let K represent the group formed by all the substitutions in the holomorph* of G which transform the substitutions of G according to its group of cogredient isomorphisms. The order of K is some power of p, and its subgroup formed by all the substitutions that omit a given letter is the group of cogredient isomorphisms of G. From the facts that each letter of this subgroup corresponds to a substitution of G,† and that this subgroup omits p^k ($k \overline{>} 1$) letters of G, it follows that G contains p^k invariant substitutions. Hence, the given theorem includes the important theorem, due to Sylow, that every group of order p^m contains invariant operators besides identity.

When G_1 is transitive, it must be holomorphic to the regular constituent of G_2 mentioned above, since G_2 contains at least one other subgroup which is conjugate with G_1 under G. As all of these conjugates are transitive, there can be only two of them. This is only possible when $p = 2$ and $k = \frac{m-1}{2}$. Hence, the

THEOREM II.—*If the subgroup formed by all the substitutions which omit one letter of a transitive group of order p^m is transitive, the order of the group is 2^{2n+1}, n being any integer.*

When the condition of this theorem is satisfied, G_2 is clearly the direct product of G_1 and its other conjugate. Hence, it follows from a known theorem‡ that the number of transitive substitution groups of order 2^{2n+1}, whose largest subgroups of degree lower than the degree of the group are transitive, is equal to the number of regular groups of degree 2^n.

Since each of these groups may be constructed by writing a regular group of order 2^n in two distinct sets of letters and adding to their direct product a substitution of order two which permutes the corresponding letters of its systems of intransitivity, the number of invariant operators of such a group must be the same as the number of such operators in the mentioned regular group of order 2^n. The largest Abelian subgroup that is contained in such a group is clearly the

* Bulletin of the American Mathematical Society, vol. VI, 1900, p. 396.

† Ibid., vol. V, 1899, p. 245.

‡ Quarterly Journal of Mathematics, vol. 28, 1896, p. 207. American Journal of Mathematics, vol. XXI, 1899, p. 306.

direct product of the Abelian subgroups of these regular groups of order 2^n. Hence, the transitive groups of order p^m in which the subgroup formed by all the substitutions which omit a given letter is transitive, constitute an infinite system of groups of order 2^{2n+1} which are completely determined by the groups of order 2^n.

Suppose that G_1 contains k systems of intransitivity. The number of systems of intransitivity of G_2 is then $\overline{\gtrless} k+1$. We shall first show that $p \overline{\gtrless} k+1$. The largest subgroup of G which transforms G_2 into itself must transform G_1 into p^λ $(\lambda \overline{\gtrless} 1)$ of its conjugates, and hence it must contain $k+1-h\,(p-1)(h \overline{\gtrless} 1)$ systems of intransitivity. This proves that $p \overline{\gtrless} k+1$. When G_1 is transitive, $k=1$ and $p=2$ as was observed above.

When $p = k+1$, the largest subgroup of G that transforms G_2 into itself is transitive. Since this transitive subgroup is of the same degree as G and contains the same subgroup that omits one letter, it must be G itself. In this case G_2 contains p similar regular constituents of order α. These results may be stated as follows:

THEOREM III.—*If the subgroup formed by all the substitutions which omit one letter of a transitive group of order p^m contains k systems of intransitivity, then $p \overline{\gtrless} k+1$. When $p = k+1$, the transitive constituents of this subgroup are similar and regular.*

Cauchy proved that the symmetric group of degree n contains subgroups of order p^m, where $m = \varepsilon\left(\frac{n}{p}\right) + \varepsilon\left(\frac{n}{p^2}\right) + \varepsilon\left(\frac{n}{p^3}\right) + \ldots\ldots;\ \varepsilon\left(\frac{a}{b}\right)$ being the largest integer which does not exceed $\frac{a}{b}$.* We proceed to determine when such a group (G) is transitive and to study some of the properties of these groups. Since the symmetric group of degree n contains all the possible substitutions in n letters, G is of degree n whenever $n \equiv 0 \mod p$. The degree of each of the transitive constituents of G must be a power of p, as it is a divisor of p^m. If G were intransitive when $n = p^\beta$, we would have

$$p^{\beta_1} + p^{\beta_2} + p^{\beta_3} \ldots\ldots = p^\beta,$$

$p^{\beta_1}, p^{\beta_2}, p^{\beta_3}, \ldots\ldots$ being the degrees of the transitive constituents of G. Hence, the number of constituents of lowest degree would be a multiple of p. As these constituents would all be similar, we could combine p of them and thus form a

*Cauchy, Comptes Rendus, vol. 21, 1845, p. 844.

transitive constituent of a larger order in the same letters. This is impossible, as $n!$ is not divisible by p^{m+1}. G must, therefore, be transitive when $n = p^\beta$.

It is clear that all the symmetric groups of degrees $p^\beta + \alpha$, $\alpha < p$ contain the same G, and that the G's of all the symmetric groups of degrees $p^\beta + \alpha'$, $\alpha' < p^{\beta+1} - p^\beta$ are the direct products of this G and the G of the symmetric group of degree α'. That is, when α' is $p^\beta\,(p > 2)$, the corresponding G is the direct product of the G of the symmetric group of degree p^β and its conjugate written in a distinct set of letters; when $\alpha' = 2p^\beta\,(p > 3)$, the corresponding G is the direct product of three such groups; when $\alpha' = lp^\beta + j\,(p > l + 1, j < p^\beta)$ the corresponding G is the direct product of $l + 1$ such groups and the largest group whose order is a power of p that is contained in the symmetric group of degree j. Hence, the

THEOREM IV.—*The largest group G of order p^m that is contained in the symmetric group of degree n is transitive whenever $n = p^{m'} + \alpha$, $\alpha < p$, and only then. When this condition is satisfied, G contains a subgroup of order p^{m-1}, which is the direct product of p conjugate transitive groups of order $p^{\frac{m-1}{p}}$. These transitive groups in turn contain subgroups of order $p^{\frac{m-1}{p}-1}$, which are the direct products of p conjugate transitive groups of order $p^{\frac{m-p-1}{p^2}}$, etc.*

COROLLARY I.—*In a group of order p^m, every subgroup whose order exceeds p^{m-n-1} $(m > p^{n-1} + p^{n-2} + \dots + 1)$ is invariant or contains an invariant subgroup of order $\overline{\gtrless}\, p$.*

COROLLARY II.—*The largest subgroup of order p^m that is contained in any symmetric group contains just p^γ invariant operators, γ being the number of its transitive constituents.*

This theorem was proved above. To see that it involves Corollary I it is only necessary to observe that a group of order g which contains a subgroup of order g_1, which is not invariant nor contains an invariant subgroup of the entire group, can be represented as a transitive substitution group of degree $g \div g_1$.* Corollary II follows from the fact that each of the transitive constituents of the mentioned subgroups of order $p^{\frac{m-1}{p}}$ contains just p invariant operators.

We proceed to give a method by means of which it is possible to construct a transitive group of order p^m (m being any number greater than 2) which con-

* Dyck, Mathematische Annalen, vol. XXII (1883), p. 102.

tains only p invariant operators. Let H represent a regular group of order p^α which contains only p invariant operators and whose quotient group with respect to these invariant operators contains no operator whose order exceeds p, and let H_1 be the conjugate of H which is formed by all the substitutions (in the same letters as are contained in H) which are commutative with every substitution of H.* Since the quotient group of H_1 with respect to its p invariant operators contains no operator whose order exceeds p, H_1 contains a non-Abelian subgroup of order p_3 which includes its p invariant operators. This subgroup and H generate a group of order $p^{\alpha+2}$ which contains only p invariant operators with respect to which its quotient group contains no operator whose order exceeds p. Since it is well known that groups of the given type exist when $\alpha = 3$ or 4,† it follows that they exist for every value of $\alpha > 2$.

It follows from the preceding paragraph that the only value of m for which a group of order p^m must contain more than p invariant operators is two. It is easily seen that this is also the only value of m for which every subgroup of order p^{m-2} is invariant; for if a group of order p^α contains a non-invariant subgroup of order $p^{\alpha-2}$, any direct product of which this group is a factor must have the same property. Since groups of order p^3 contain non-invariant subgroups of order p, there must be groups of order p^m (m being any integer > 2) which contain non-invariant subgroups of order p^{m-2}.

The following method may be employed to determine all the groups of order p^m, provided all the groups of order p^{m-1} are known. Suppose that a group (R) of order p^m is represented as a regular group. Any one of its subgroups (H) of order p^{m-1} contains p systems of intransitivity which are permuted according to the group of order p by the remaining substitutions of R. Hence, H may be constructed by writing after each substitution of a regular group of order p^{m-1} the same substitution in $p-1$ distinct sets of letters.‡ All of the other substitutions of R are of the form st, where t merely interchanges the corresponding letters of the p systems of H and s transforms each one of these systems into itself.§

Since t is completely determined by H, it is only necessary to consider how s may be selected. When the substitutions of H are transformed by R

* Jordan, "Traité des substitutions," 1870, p. 60.

† Hölder, Mathematische Annalen, vol. XLIII, 1893, p. 410.

‡ Quarterly Journal of Mathematics, vol. XXVIII, 1896, p. 236.

§ Ibid.

according to a substitution in its group of cogredient isomorphisms, we may assume that s is commutative with each substitution of H. In this case it may evidently be assumed that s involves only the letters of the first system of intransitivity of H, for, if it were otherwise, we could transform st by a substitution which would transform H into itself and also reduce the number of letters in s. Hence, there cannot be more such groups than the number of sets of substitutions in H which are conjugate under its holomorph. This number may sometimes be reduced by the following considerations:

Let $s_1, s_2, s_3, \ldots, s_p$ represent the constituents of a substitution of H, each constituent involving all the letters of one of the transitive constituents of H. From the equations

$$\begin{aligned}(s_1^{p-1}s_3 s_4^2 s_5^3 \ldots s_p^{p-2})^{-1} t s_1^{p-1} s_3 s_4^2 s_5^3 \ldots s_p^{p-2} \\ = (s_1^{p-1}s_3 \ldots s_p^{p-2})^{-1} t s_1^{p-1} s_3 \ldots s_p^{p-2} t^{-1} t = s_1^{1-p} s_2 s_3 s_4 \ldots s_p t,\end{aligned}$$

it follows that s may be so selected that it is not the p^{th} power of any substitution in the first transitive constituent of H. Since s must clearly be commutative with every substitution of H, none of the powers of a non-commutative substitution in the first transitive constituent of H is a suitable value of s. In particular, we observe that s can have only one value when H is cyclical or when it is Abelian and of type $(1, 1, 1, \ldots)$. It has been assumed throughout that s' is not identity, and that R transforms H according to a substitution in its group of cogredient isomorphisms.

When some substitutions of R transform H according to a substitution which is not in its group of cogredient isomorphisms, we may write these substitutions in the form st_1t, where t_1 and t are commutative, while s is commutative with every substitution of H. As in the preceding case, we may assume that s involves only the letters of the first transitive constituent of H, and hence it is also commutative with t_1. It is evident that t_1 may be restricted to at most one out of each conjugate set of operators of order p^β in the group of isomorphisms of H.

CORNELL UNIVERSITY, *Dec.*, 1900.